Amendments to the Specification

Please replace the paragraph on page 1, line 19 to page 2, line 5 with the following amended paragraph:

Businesses have a need for exchanging computer-based data with each other[[.]] ([[E]] e.g., manufacturers need to order parts from suppliers, vendors need the ability to maintain their products on customer networks, and management service providers need to maintain computing equipment on customer networks[[.]]). Originally voice communications, facsimile, e-mail or direct contact was used to exchange such data. More recently, advanced network techniques have allowed parties to communicate more directly by dedicated computer networks[[:]], thereby eliminating more costly solutions.

Please replace the paragraph on page 2, lines 11-13 with the following amended paragraph:

As technology has moved business networking from private to shared private to virtual private networks, the reoccurring cost of the connection has decreased; however, new disadvantages have surfaced:

Please replace the paragraph on page 3, lines 11-12 with the following amended paragraph:

(d) a method by which the establishing party of a temporary directed circuit[[s]] may be authenticated and authorized;

Please replace the paragraph on page 8, lines 1-3 with the following amended paragraph:

FIG. 9 is a block diagram depicting configuration and status objects for domain[[s]] appliances and passively monitored devices and their relationships using the unified object-oriented methodology notation;

Please replace the paragraph on page 12, lines 3-10 with the following amended paragraph:

While many features of the present invention can be created with a similar set of separate or existing routers, firewalls and VPN hardware on each of the private networks, such a solution requires potentially greater capital expense since more equipment is involved and certainly greater operational expense to configure and maintain the more abstract notion of policy in the form of specific configuration rules on multiple pieces of network apparatus. Thus one of the markedly distinguishing ~~capability~~ capabilities of the present invention is in the ability for the appliances 114, 116 to effect policies in an automated fashion.

Please replace the paragraph on page 12, line 22 to page 13, line 6 with the following amended paragraph:

Although traditional VPN technologies such as Point to Point Tunneling Protocol and IPSEC may be leveraged to form the carrier tunnel, essentially any tunneling technology may be used with respect to the present invention[[:]] including proprietary methods. This is due to the fact that the carrier tunnel is part of a closed solution[[:]] not intended to extend or leverage existing VPN deployments in any way. There are many different types of tunneling and many different ways of implementing tunneling and it is the notion of the carrier tunnel that is germane to the present invention. The actual tunneling technology utilized is left up to the person skilled in the art.

Please replace the paragraph on page 13, lines 7-13 with the following amended paragraph:

Referring to FIG. 3, as noted above, the appliance 114 in the ~~directornetwork~~ director network contains a tunnel server 122. The appliance 116 on the second (satellite) network contains a tunnel client 120. At this level, there is the potential for a carrier tunnel 118 to be established between the two appliances over the public network 100. By introducing a network filter and packet router 126 on each appliance 114, 116 it is possible to effect a directed circuit 124 that further refines the constraints of the tunnel 118 to suit the requirements of previously agreed upon previously established policies of engagement.

Please replace the paragraph on page 14, lines 5-15 with the following amended paragraph:

A protocol probe 136 on the remote appliance 116 will periodically send protocol requests 138 to a network entity 112. Information collected by the probe will be stored in a protocol cache 140. On a periodic basis, the heartbeat generator 142 will collect information about the state of the appliance 116 and information from the protocol cache 140 to build a heartbeat response. This response is an XML document that ~~in~~ is transferred to the heartbeat monitor application 146 within the controller 128 via the HTTP protocol. The heartbeat monitor application 146 is then able to update the controller's database 148 with current information about the status of the remote application 116 and the remote network entity 112. Subsequently, an end-user of the controller 128 may use a workstation 134 to access information from a remote network management proxy 152 on the controller 128 via a protocol request 150.

Please replace the paragraph on page 15, lines 7-20 with the following amended paragraph:

Referring to FIG. 7, several objects are used within the controller to track end-user authentication. The UserBean 162 represents an end-user with rights on the controller. Each user may have many sessions with the controller with the potential of accessing the controller from multiple ~~workstation~~ workstations at the same moment[[,]]. [[e]]Each of these sessions is tracked by a SessionBean 164, which associates the session with the IP address of the workstation and the UserBean 162. Each directed circuit is represented by a DirectedCircuitBean 166. Each user may have many directed circuits. A session and/or a workstation's access to a given directed circuit is determined by the relationship of a UserBean 162 to its relationship with many SessionBeans 164 and many DirectedCircuitBeans 166. Each carrier tunnel is tracked by a TunnelBean 168. Each TunnelBean 168 is associated with many DirectedCircuitBeans 166 and each DirectedCircuitBean is associated with one TunnelBean 168. Via these relationships directed circuits and their carrier tunnels are related back to the workstations used by them.

Please replace the paragraph on page 15, line 21 to page 16, line 2 with the following amended paragraph:

The controller must have a local appliance to participate in directed circuits[[,]]. ~~since~~ Since this appliance will typically listen for incoming tunnel requests, we refer to it as the server appliance. Referring to FIG. 8A, both the server appliance 114 and the client appliance 116 send heartbeat messages to the controller 128 on a periodic basis. Upon receipt of the heartbeat message, the controller 128 will respond with a request message.

Please replace the paragraph on page 16, line 14 to page 17, line 3 with the following amended paragraph:

Referring to FIG. 9, several objects are used by appliances and the controller to represent the aforementioned response elements within their respective database and distributed state-machine components. The DomainBean 184 describes a domain and serves as ~~a~~ an aggregation point for a single DomainStatusBean 190 and many ApplianceBeans 186. While in the response protocol only one appliance is preferably associated with a given domain, a controller may associate many appliances with a given domain. The ApplianceBean 186 is an aggregation point for one ApplianceStatusBean 192, many LogBeans 194 and many DeviceBeans 198. The LogBean 194 is an aggregation point to many LogEntryBeans 196 which describe deltas to log entries on the appliance. The DeviceBean 198 describes a device that may potentially participate as a network entity in a directed circuit and serves as an aggregation point for a single DeviceStatusBean 200 and many DeviceProtocolBeans 202. The DeviceProtocolBean describes the state of a particular protocol associated with the given device.

Please replace the paragraph on page 21, lines 11-13 with the following amended paragraph:

Once the controller 128 has been notified by both the client 116 and server 114 that a directed circuit has been closed, the ~~control~~ controller 128 will send a log directed circuit down message to the audit database 214.